面向SaaS的商用密码统一服务平台设计

梁　坤

（中国移动通信集团湖南有限公司，湖南长沙 410001）

【摘要】文章提出一种面向SaaS的商用密码统一服务平台设计方案。通过该方案构建的平台，实现高度整合统一的密码资源，直接面向移动信息系统业务应用场景，提供统一的用户管理、统一身份认证、统一的密码规范、密码运算接口和密码运维管理等全面的密码业务支撑服务，支持移动信息系统基于商密算法的安全升级，满足信息系统的商用密码应用、安全性标准要求和政策要求。

【关键词】统一密码服务；身份认证；数据安全；数据脱敏

【doi:10.3969/j.issn.2095-7661.2022.02.009】

【中图分类号】TP309　　【文献标识码】A　　【文章编号】2095-7661(2022)02-0032-05

Design of SaaS-oriented Commercial Cryptographic Algorithm Comprehensive Service Platform

LIANG Kun

（China Mobile Group Hunan Co., Ltd., Changsha, Hunan, China 410001）

Abstract: This paper proposes a design scheme of SaaS - oriented commercial cryptographic algorithm comprehensive service platform. Through the platform constructed by the scheme, the highly integrated and unified cryptographic resources are realized, which directly face the mobile information system business application scenarios and provide comprehensive cryptographic support services such as unified user management, unified identity authentication, unified cryptographic specification, cryptographic operation interface and cryptographic operation and maintenance management to support the security upgrade of mobile information system based on commercial cryptographic algorithm, meet the requirements of commercial cryptographic application and security standards and policies of information system.

Keywords: unified cryptographic service; identity authentication; data security; data desensitization

1 研究背景

近年来，我国逐步完善网络安全相关法律法规、安全标准，出台了《网络安全法》《密码法》《数据安全法》《个人信息保护法》等，要求使用商用密码算法对数据进行保护[1]。随着等级保护2.0和密码应用安全性评估的相关政策标准施行，数据安全防护已经成为了信息系统运营方的责任和义务[2]。

与此同时，电信行业下发的《2021年基础电信企业行业数据安全标准贯标工作方案》明确要求加强行业内数据安全管理水平[3]，建立健全数据安全管理制度，实施数据分类分级，制定重要数据清单，完善数据安全防护技术措施，提升数据安全保护能力。

目前企业内部各个业务系统中存在大量数据，数据的采集、传输、存储、访问、使用、汇聚等各个环节都可能存在安全风险，根据业务现状和需求，需进行商用密码算法改造[4]，对敏感数据进行加密保护，保证业务数据的安全，同时进行密码应用安全性评估，以符合政策要求。

目前的商用密码改造方式是给每一个业务系统配备独立的密码基础设施，多个业务系统就需要多套，而有些密码基础设施的利用率又不够高，

[收稿日期] 2022-05-05

[作者简介] 梁坤(1976-)，女，湖南长沙人，中国移动通信集团湖南有限公司信息安全管理部副总经理，硕士，研究方向：网络及数据安全规划。

造成严重的资源浪费；另外各个密码厂商接口不统一、不规范，导致开发调用复杂，改造困难。

因此迫切需要建设面向SaaS且采用商用密码算法的统一服务平台，为移动业务系统提供统一的密码基础设施以及统一的密码服务和支撑能力，形成体系化的统一标准接口，进而实现以下目标：满足相关政策规范要求，推进商用密码技术安全合规应用；使用商用密码算法对数据和网络进行保护以满足企业的现实需求；采用节约开发、减少建设及运维成本的集约化建设，确保信息平台整体安全提升的合理可行。

2 商用密码统一服务平台架构设计

本文提出一种面向SaaS的商用密码算法统一服务平台（以下简称“密码统一服务平台”）设计方案。通过采用密码资源池化技术、构建安全接入平台、提供统一身份认证和数据安全服务，为企业各业务系统提供全面的密码服务支撑；通过提供灵活、多样、标准的密码服务接口，高效地保障移动业务应用与业务数据的安全。

2.1 设计原则

1）标准性和开放性。充分考虑“标准和开放”的原则[5]，支持各种相应的软硬件接口，使之具有灵活性和延展性，具备与多种系统互连互通的特性，在结构上实现真正开放，便于与其它系统的互联和扩展，使得平台具有可移植性、互操作性。

2）适用性和可扩展性。具备良好可扩展性，能够随着应用的变化和用户的增加不断地进行扩展。同时充分考虑了各个功能模块的可重复利用，降低了系统扩展的复杂性，增强系统的弹性、通用性与可替换性。

3）组件化设计。采用了组件化的设计思想，通过采用统一的标准接口规范，方便今后扩展和添加其他子系统，同时增加系统的可维护性和易扩展性[5]。

4）自主可控，安全合规。基于国产密码SM2/3/4/9算法，从身份认证、网络安全、数据使用与存储安全等方面进行综合防护。采用并支持多种具有商密产品型号的设备、产品，确保密码算法使用的正确性和密码应用的合规性。

5）高可靠/高安全性原则。使用安全和可靠的商用密码体系，使平台具有高可靠性。采用负载双活机制确保平台服务不中断，保证在发生事件或灾难时，能够提供不间断的密钥运算服务。

2.2 架构设计

密码统一服务平台在架构设计时遵循国家相关安全规范，满足信息系统的商用密码应用及安全性标准要求[1]。平台包括应用服务层、接口服务层和资源服务层，以及对应的功能与管理模块，如图1所示。

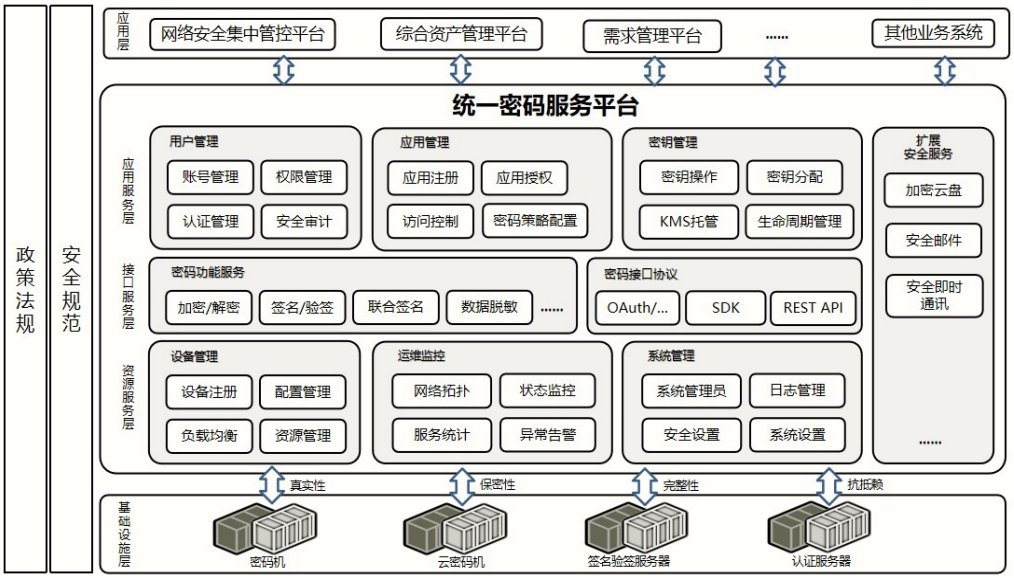

图1　密码统一服务平台架构图

1）应用服务层，提供统一用户管理、应用管理和密钥管理等功能模块，以及可选配的安全服务组件。

2）接口服务层，针对目前主流的B/S应用和C/S应用，提供统一密码功能调用SDK/API接口，业务系统应用服务通过调用各种密码算法接口，通过服务平台密码资源服务能力实现各种密码运算，进行数据/数据库加密、数字签名及签名验签等操作。接口支持多种主流接入方式和身份认证协议，并可支持SDK/API定制；另外提供安全中间件，通

过安全中间件集成模式可实现定制化的数据库加密服务，由业务系统开发者基于密码统一服务平台的密码服务接口进行集成开发。

3）资源服务层，提供统一设备管理、运维监控和系统管理等功能模块，实现对平台的整体运行配置、管理、监控和审计等功能。

4）基础设施层，使用密码机、签名验签服务器、身份认证服务器为应用提供最为基础和底层的密钥管理和密码计算服务，支持国产密码算法SM2/3/4/9。

3 密码统一服务平台功能设计

3.1 功能设计框架

根据上述的架构设计，密码统一服务平台是密码设备硬件基础设施和平台软件组成的软硬件结合的形态。其中密码设备基础设施提供密码运算能力，平台软件提供密码能力服务，并对上层业务提供统一密码服务。平台软件包括数据安全服务系统、统一身份认证系统、统一安全接入系统、统一密码资源服务系统等软件组成，功能设计框架如图2所示。

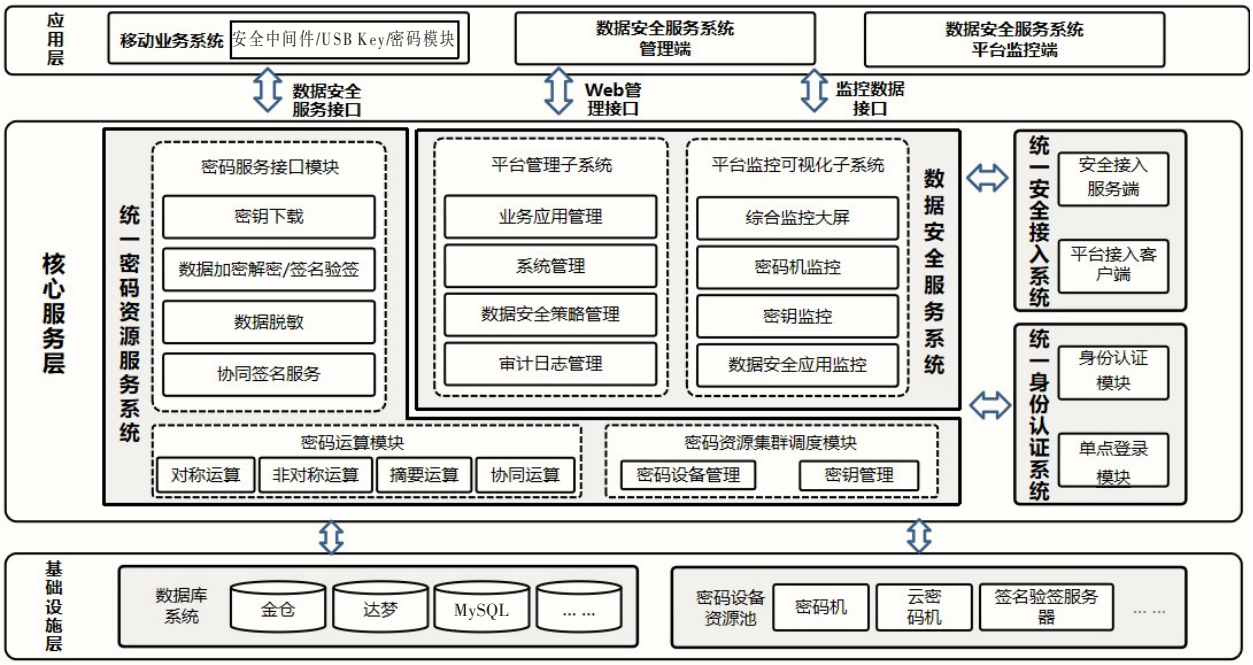

图2 功能设计框架图

3.2 主要模块功能设计

3.2.1 统一安全接入系统

安全接入系统实现用户端与密码统一服务平台、业务系统之间数据安全加密传输，采用国产密码算法实现密码统一服务平台对接入用户的身份认证，并支持基于IP、端口、账号等设置详细的访问控制。主要的功能如下：

1）安全接入系统服务端：采用基于TLCP协议、SM9密码技术为核心实现身份认证、安全接入、加密传输。服务端同时具备SSL VPN使用简单和IPSEC VPN应用透明的特点，用户可以在各种环境中实现远程安全接入进而安全访问内部网络各种应用。

2）安全接入客户端：支持Windows、Android、iOS系统各类型终端，提供密钥下载、与接入系统服务端建立安全通道的功能。提供安全接入SDK，可与应用系统客户端程序集成，实现无需独立安装即可安全接入。

3.2.2 统一身份认证系统

统一身份认证系统采用商用密码技术提供包括扫码、短信、USB Key等多种方式的身份认证功能，再通过构建单点登录认证服务，提升用户登录业务系统的体验。主要功能包括：

1）采用SM9标识密码技术，采用SM9标识密码算法进行统一身份认证与管理，手机号/系统账号即为标识公钥，简化了身份密钥管理流程。

2）用户访问连接服务端系统时，采用SM9算法完成挑战应答认证过程，无需口令登录，服务端也无需存储用户口令。

3）安全登录网关可拦截所有访问应用系统的请求，检查是否带了访问应用系统的合法token值，通过判断将合法请求提交认证，对非法请求进行拦截阻断。

4）用户登陆PC端业务系统时，可以用用户名或扫码登录、短信登录、USB Key登录等多种方式实现安全快速的身份认证，其中扫码登录时不再

使用USB Key，改为使用手机App的扫码，即不使用硬件介质，在Android和iOS系统中基于密码软件模块实现终端用户密钥的安全存储和安全使用。

5）单点登录，为终端用户访问各服务系统提供一键认证登录功能，无需用户重复输入不同系统的认证信息，简化用户访问应用系统的操作使用流程。单点登录服务器支持使用灵活的配置来满足不同级别身份认证的安全需求，保证用户登录系统的合法性、便利性。

3.2.3 数据安全服务系统

数据安全服务系统包括数据安全服务管理子系统和数据安全服务监控子系统。其中数据安全服务管理子系统为业务应用使用密码服务提供平台支撑，包括数据安全策略管理模块、系统模块、业务应用管理、日志审计等模块；数据安全服务监控子系统将资源的使用情况、密码服务的运行状态、业务应用的密码服务调用统计实时监控通过监控大屏动态展示。

1）数据安全服务管理子系统

数据安全策略管理模块，主要功能包括：提供源数据管理、数据安全分级、数据权限管理、敏感范围管理、敏感数据地图等管理功能，提供数据安全策略支撑服务；建立数据分布地图，构建数据访问权限体系，实现敏感数据标记和数据分类，梳理数据安全需求，为数据加解密等安全服务提供具体策略实施依据。

系统管理模块，支持管理员管理、角色权限管理、管理员认证配置、参数配置等功能。管理员管理包括：增加、锁定、解锁、删除、注销等管理。角色权限管理：角色分为超级管理员、系统管理员、业务管理员、审计管理员。管理员认证配置，配置分为管理员认证方式配置、多因子认证方式配置、认证规则配置、登录控制。

业务应用管理模块，通过业务应用管理功能对新增的业务应用及所在机构的信息、资源、认证以及服务进行管理。业务应用信息管理：设置业务应用及所在机构相关信息，如业务应用名称、机构名称、机构类型等。业务应用资源管理：配置服务资源（最大用户数、分配密钥数）。业务应用认证管理：配置认证类型、传输协议、应用ID以及应用凭证（API访问密码）等。业务应用服务管理：设置服务启用、禁用状态。

日志审计模块，构建一体化日志审计，收集、整合基础资源平台、网络连接设备、主机操作系统、数据库系统、数据访问使用、应用服务系统、终端用户行为等各个来源的操作日志，进行标准化处理后统一汇聚存储，形成完整的审计日志数据库，对内部业务系统日志进行实时审计，保障安全事件有据可查。主要功能包括：日志采集，通过Syslog、SNMP、NetFlow、ODBC/JDBC等协议采集日志，支持从Log文件或者数据库中获取日志，日志采集的范围和采集信息的颗粒度可自定义进行调节；日志分析，对于采集的信息进行分析、审计，采用基于规则、时序的审计等，提供多样化的实时告警手段，发现安全问题应及时告警，提供符合自身需求自定义报表的功能；日志存储，对于采集到的原始信息，以及审计后的信息都要进行保存、备查，并可以作为取证的依据，对原始日志数据进行加密存储，确保其不被删除、更改、破坏、非法访问，为安全事件证据追查、第三方安全测评等提供真实依据。

2）数据安全服务监控子系统

运维监控模块提供对上层业务应用密码使用情况、下层密码基础设施运行状况进行监控和数据统计功能。监控内容包括密码资源的使用情况、密码服务运行状态、异常告警处理、业务应用密码服务使用情况统计、资源使用趋势预警等，并提供丰富的可视化视图。

3.2.4 统一密码资源服务系统

统一密码资源服务系统为移动业务应用系统提供基于商用密码算法的技术支撑，也为后续的各种信息化应用提供了基于商用密码算法的多种服务能力。统一密码资源服务系统是包含密码服务、密钥管理、密码设备管理等功能，由密码服务接口模块、密码运算模块、密码资源集成调度模块组成。

1）密码资源调度模块

对内实现对密码机、云密码机、签名验签服务器等密码资源进行创建、管理、调度、迁移、销毁等全生命周期进行管理，对用户、应用进行管理，对外提供用户密码资源审批服务和用户已申请资源的管理服务。密码设备管理：支持添加不同厂商的密码设备，支持查看每台设备的24小时运行概况，支持对设备的异常情况进行告警。密钥管理：通过密钥资源池对已存在的密钥进行管理，可启用或停止密钥服务、检测密钥被调用是否正常以及显示密钥资源池可用数量、总数量、已使用数量；通过密钥管理对多种密钥算法类型的密钥进行管理，可设置创建密钥的类型、数量及密钥策略，按机构对密钥进行分组，密钥创建权限控制保障应

用间密钥数据权限隔离。

2)密码运算模块

提供支持SM2/3/4/9全系列国产密码算法的密码计算。以接口形式向业务客户端提供非对称加解密运算、对称加解密运算、签名验签运算、数据摘要运算、联合签名/解密运算等密码服务接口。

3)密码服务接口模块

密码服务系统以接口形式对外统一提供密钥调用、密码运算服务,向业务客户端提供密钥对生成、存储和使用安全保护,安全SDK/API支持C、C++、JAVA等多种开发语言,可应用于Android、iOS、Linux等多种系统平台。数据加解密、签名验签:业务系统采用接口调用或SDK接口方式集成,调用API/restful接口或SDK接口的方式集成到业务系统中,实现业务系统调用密码能力进行敏感数据的加解密或签名验签。协同签名:协同签名通过密钥分割技术,能够保证在不重现完整私钥的前提下完成数字签名操作,从而规避了私钥被恶意程序直接跟踪截取的风险,以接口方式向终端提供联合数字签名响应服务,在校验终端用户身份的合法性后提供SM2、SM9私钥的协同签名等功能。数据脱敏:支持静态/动态、在线/离线数据脱敏,数据脱敏后保持原有数据的格式,支持脱敏数据的在线受控还原,支持生成系统对数据的实时在线处理;支持数据脱敏加密密钥的分隔,允许系统和用户各自拥有加密密钥,只有用户和系统共同允许才可对相关数据进行脱敏和还原。

其中,数据脱敏由管理模块和脱敏中间件构成,调用密码机的密钥和算法运算。管理模块支持多种的脱敏规则管理,脱敏中间件支持灵活的安全策略和批量数据脱敏、还原处理。主要功能如下:数据脱敏,采用标准算法SM4和安全的格式保留加密模式FF1、FF3组合对敏感数据进行加密,支持多种数据格式的格式保留加密,加密密文与明文格式相同,支持灵活的自定义数据格式;数据还原,对脱敏后的数据进行受控解密还原以恢复原始数据,进行使用;脱敏密钥分布式管理,支持按用户角色、属性配置数据脱敏过程的加密密钥,以实现按策略对敏感数据的访问控制。

3.3 网络部署设计

如图3所示,通过部署密码统一服务平台的统一密码资源服务系统、统一身份认证系统、统一安全接入系统、数据安全服务系统,可为终端接入、用户访问、应用授权、敏感信息保护、日志审计等提供全面的基于商用密码的数据安全服务。

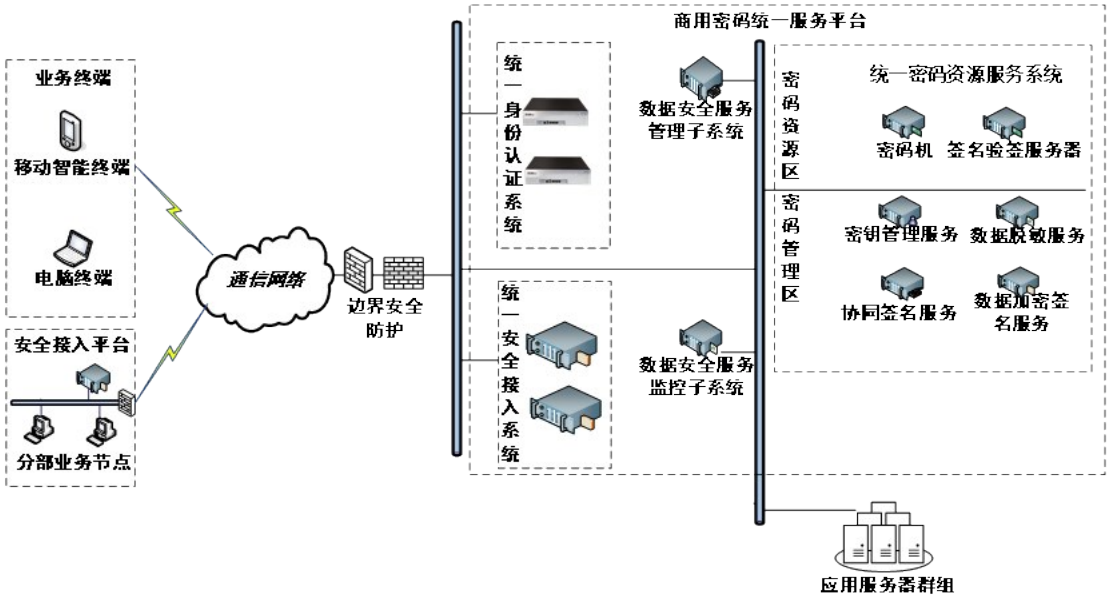

图3　网络部署拓扑图

4 结束语

根据企业业务系统的密码应用需求,本文提出面向SaaS的商用密码算法统一服务平台方案,对密码资源进行集群化管理,支持弹性扩容和动态调整,灵活分配调度业务系统中使用的密码服务资源,使密码资源在满足应用需求的同时得到充分、合理利用,有效地解决基础设施重复建设问题,极大地减少密码资源管理和运维成本。方案的创新点有:一是安全接入和身份认证流程都支持在各种终端上使用SM9标识密码算法(包括SM9协同签名算法),用户无须申请和交换数字证书,这将极大降低证书与密钥管理的　(下转第43页)

基于PLC的加工中心自动换刀控制系统设计

潘晓贝[1,2]

（1.河南省高校节能照明工程技术研究中心，河南三门峡 472000；
2.三门峡职业技术学院，河南三门峡 472000）

【摘要】文章针对加工中心的换刀系统展开研究，设计了一款立式加工中心自动换刀机械手装置，硬件设计包括刀库设计、机械手设计和PLC系统设计，软件设计包括选刀程序设计、刀库定位、换刀程序和人机界面，并以PLC为控制核心将整个过程进行了优化。研究表明，该自动换刀装置解决了实际生产中低效率的问题，有一定的参考和借鉴价值。

【关键词】PLC；机械手；刀库；步进电机
【doi:10.3969/j.issn.2095-7661.2022.02.010】
【中图分类号】TG659　　【文献标识码】A　　【文章编号】2095-7661(2022)02-0037-03

Design of Automatic Tool Change Control System of Machining Center Based on PLC

PAN Xiao-bei[1,2]

(1. Henan University Energy-saving Lighting Engineering Technology Research Center, Sanmenxia, Henan, China 472000; 2. Sanmenxia Polytechnic, Sanmenxia, Henan, China 472000)

Abstract: This paper studies the tool change system of the machining center and designs an automatic tool change manipulator device of the vertical machining center. The hardware design includes tool magazine design, manipulator design and PLC system design. The software design includes tool selection program design, tool magazine positioning, tool change program and man-machine interface. The whole process is optimized with PLC as the control core. The research shows that the automatic tool changing device solves the problem of low efficiency in actual production and has a certain reference value.

Keywords:PLC; manipulator; tool magazine; stepper motor

数控机床在进行自动加工时，要在不同的加工工艺及方法之间进行多次切换刀具，例如车、铣、刨、磨、钻等，若采用人工更换刀具，则必定增加工件加工时间。如果将换刀时间缩短，机床的加工效率将极大提高。因此许多厂家都投入大量的时间、精力和资金研制柔性的自动换刀装置，以代替人工进行自动、可靠、高效的换刀操作。当机床需要换刀时，自动换刀装置会从刀库中选取所需的刀具安装到主轴上，同时把主轴上的刀具取下放回刀库中。整个换刀过程效率提高，错误率降低，对刀具也是一种保护[1]。自动换刀装置可以在高节拍连续换刀的工作要求下缩短刀具更换及停机占用的时间，降低了机床操作工人的劳动强度和重复换刀工作时的心理疲惫。所以，为了充分适应我国现代化机械制造工业技术不断发展表现出的各种现实应用需求，加工制造中心应装设自动换刀装置[2]。

1 整体控制方案设计

根据要求分别从硬件和软件两个方面对自动换刀装置的各个部分进行设计。硬件设计包括：刀库设计、机械手设计和PLC系统设计，其中PLC系统设计包括硬件选型和驱动方式的确定。软件设

[收稿日期] 2022-04-18
[作者简介] 潘晓贝(1982—)，女，河南灵宝人，三门峡职业技术学院副教授，工程硕士，研究方向：自动化技术应用、传感检测技术。
[基金项目] 2021年度三门峡职业技术学院院级科研项目“基于PLC的加工中心自动换刀控制系统研究与设计”(项目编号:SZY-2021-001)。

计包括：选刀程序设计、刀库定位、换刀程序和人机界面。整体方案设计如图1所示。

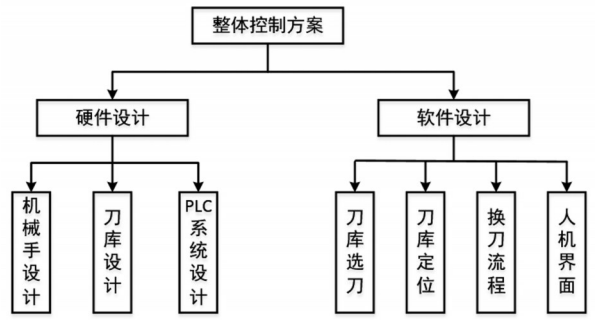

图1 整体方案设计结构图

2 硬件设计

2.1 刀库结构设计

刀库主要有圆盘式、链式、转塔式、斗笠式等。随着各种刀库类型的应用，机床多采用圆盘式刀库结构。圆盘式刀库也叫盘式刀库，通常被广泛应用在立式切削加工中心。圆盘式刀库整体尺寸不会太大，直径一般在1米左右，这种刀库需要使用换刀机械手配合完成换刀过程。需要换刀时，刀库的驱动装置按照PLC指令旋转相应的角度，使主轴需要的刀具正对机械手夹爪夹取刀具的位置，并将刀套翻转，使机械手能够夹紧刀具，之后机械手旋转180°，将所需刀具换位，完成刀具的替换。圆盘式刀库结构外形如图2所示[3]。

图2 圆盘式刀库结构外形图

2.2 换刀机械手设计

对于自动换刀装置而言，目前大多采用机械手来更换刀具。机械手换刀时不仅灵活性大并且具有柔性加工特性，适用广度更大，效率更高，可以充分应用于各种柔性加工场合中。目前各种加工中心自动换刀所用的机械手常用的是双臂双爪回转式换刀机械手，如图3所示。双臂机械手有两个在一条直线上的机械手臂，其回转机构在两个手臂之间，每个手臂端各有一个夹爪，两个抓刀手在加工过程中都可以进行装刀和卸刀，通过旋转180°来替换主轴上的刀具。换刀时，机械手同时抓住主轴上暂时不用的刀具和刀库中需要使用的刀具向下运动，旋转180°，交换刀具，再把机械手向上提起，使两把刀具运动到位，再把刀具夹紧，完成换刀[4]。

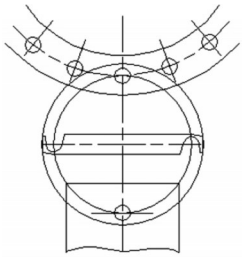

图3 双臂双爪回转式换刀机械手

2.3 PLC控制系统设计

2.3.1 PLC选型

本设计选择西门子1200PLC作为主要控制器。S7-1200采用了一种模块化的结构设计，可以同时满足多种工作场所的要求，并且它们能够很好地实现各种自动化场合。S7-1200具备200系列的各种功能，又添加了许多全新的实用功能，可以适应更广阔的专业应用领域。S7-1200具有强大的频率测量闭环控制以及频率运动闭环控制等核心功能，拥有一个集成多达六个高速计数器，使其同时能够被用来精准地实时监视多个编码器的高速频率运动计数，或者对运算过程中可能发生的复杂事件实时进行高速频率计数。

2.3.2 PLC控制系统I/O地址的分配

控制系统中PLC的输入信号有：启动、停止、自动/单步、刀库定位、刀具计数、刀库刀套翻转、主轴松刀、主轴紧刀、机械手旋转、机械手紧刀、机械手松刀等输入端。PLC输出信号有：刀库步进电动机正转、刀库电机反转、刀套翻转、刀套回位、机械手旋转、机械手紧刀、机械手松刀等[5]。本控制系统的I/O分配表如表1所示。

表1 PLC I/O分配表

输入端子分配	对象用途	输出端子分配	输出功能
I0.0	启动	Q0.0	电机控制
I0.1	停止	Q0.1	电机控制
I0.2	自动	Q0.2	刀库正转
I0.3	手动	Q0.3	刀库反转
I0.4	刀库定位接近开关	Q0.4	刀套翻转
I0.5	刀套翻转接近开关	Q0.5	刀套回位
I1.1	主轴松刀接近开关	Q1.1	主轴紧刀
I1.2	主轴紧刀接近开关		

3 软件系统设计

3.1 PLC程序流程设计

刀库中刀具数量和编号需要在PLC内部存储器存储。将刀库中刀具的编号下载到PLC内部存储器中，使其一一对应，可以通过PLC程序进行选刀。

选刀流程为：首先判断刀库中的刀具号是否准确，然后判断刀具是否在主轴上，最后判断刀具是否在换刀位置上，计算需要转动的角度，并旋转刀具，使其和机械手位置对应，停止旋转，选刀结束，如图4所示。换刀流程为：刀库转到位后，机械手夹具松开，然后上升夹紧需要更换的两个刀具，下降，并转动180°，上升，夹具放松，机床夹紧新的刀具，刀库夹紧换掉的刀具，如图5所示[6]。

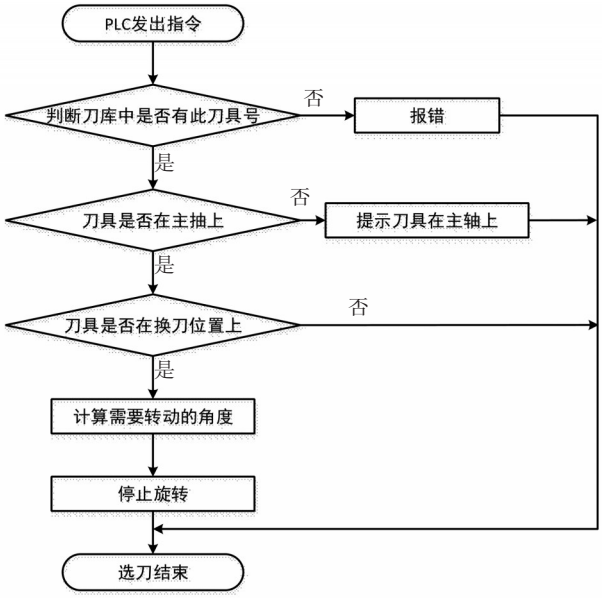

图4　选刀流程图

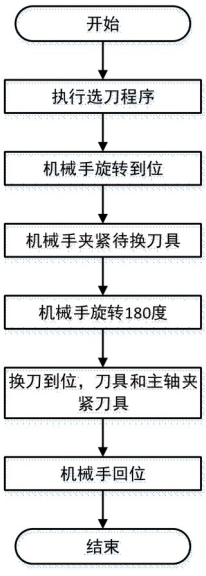

图5　换刀流程图

3.2 组态设计

本系统的人机界面使用西门子TP700精智面板，这款面板采用7英寸触摸屏，800*480像素，支持一个MRP和RT/IRT的 PROFINET/工业以太网接口（2个端口），两个多媒体卡插槽，三个USB接口。本设计使用HMI组态，与其他同类产品相比，该软件具备将数据转换为图形的特性，操作界面使用中文，极大地方便了用户使用，该触摸屏设计方便，操作简单，库图标和函数较多，使用方便。设计组态画面如图6所示，界面中可以显示机械手和刀库中的各个状态和信息，包括目标刀具和当前刀具与机械手的状态、刀套的状态、主轴的状态等信息，操作者可根据工艺要求设定目标刀具，PLC运行程序，操作者可以观测整个过程和监控各个部件的工作状态。

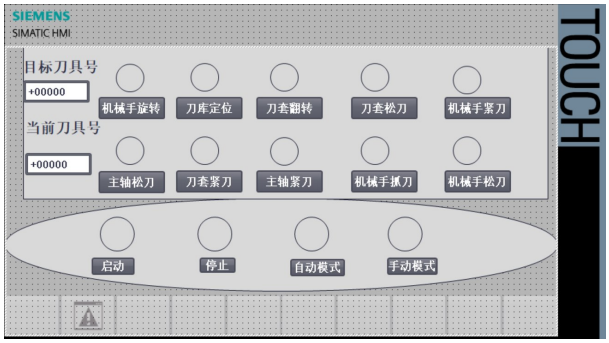

图6　组态画面

4 结语

本文设计了立式加工中心自动换刀机械手装置，实现了自动换刀功能。在设计过程中，从刀库、机械手、驱动装置三部分出发，对各部分的功能、部分结构和驱动方式进行了选型设计。对自动换刀装置的整体结构设计了一套PLC控制系统，实现刀库旋转、刀套翻转、抓刀、松刀、机械手旋转、主轴抓刀、紧刀等功能。对PLC控制部分进行了电气元件的选型，设计了选刀、刀库定位、换刀等关键步骤的流程。自动换刀装置只是能够初步进行换刀工作，解决了实际生产中的一些低效率的问题，有一定的参考和借鉴价值[7]。

【参考文献】

[1]乔志刚.基于PLC的加工中心控制设计[J].河南科技,2021(4):76-78.

[2]方亚梅.基于西门子S7-200 PLC和步进电机的自动换刀控制程序设计[J].工业控制计算机,2020(12):135-136.

[3]武永强,于涛.数控回转刀架PLC控制系统设计[J].机电技术,2020(4):54-58.

[4]朱卫国,齐琦.KUKA制孔机器人自动换刀系统设计[J].唐山学院学报,2020(6):1-5,30.

[5]王蕊,张孝元,高昆,王琪.基于PLC的刀库自动换刀控制系统设计[J].电子技术与软件工程,2018(13):110-111.

[6]梁盈富.圆盘式刀库机械手换刀的控制程序设计[J].机械设计与制造工程,2018(7):46-49.

[7]王新刚,吕春梅,赵玉倩,陈晓明.基于刀具失效率的换刀策略研究[J].兵工学报,2016(5):903-908.

基于主从同步的MySQL负载均衡设计与部署

吴锋珍

（福建水利电力职业技术学院，福建永安 366000）

【摘要】随着信息化技术的迅猛发展，为了持续为各类PC端、移动端用户提供可靠服务，数据存储的要求也发生了巨大变化，数据存储在向负载均衡、高可用性等方面发展。本研究在Linux环境下，通过MyCat为MySQL数据库配置主从同步，实现数据的读写分离，从而实现服务器的负载均衡。同时，在教考分离平台中，配置一主两从的部署方式，读写分离的优势明显，效果显著。

【关键词】MySQL；主从同步；负载均衡；高可用性

【doi:10.3969/j.issn.2095-7661.2022.02.011】

【中图分类号】TP311.13 【文献标识码】A 【文章编号】2095-7661(2022)02-0040-04

Design and Deployment of MySQL Load Balancing Based on Master-slave Synchronization

WU Feng-zhen

(Fujian College of Water Conservancy and Electric Power, Yong'an, Fujian, China 366000)

Abstract: With the rapid development of information technology, in order to continuously provide reliable services for all kinds of PC and mobile users, the requirements of data storage are also changing greatly. Data storage is developing towards load balancing and high availability. Under the Linux environment, the master-slave synchronization is configured for MySQL database through MyCat to realize the separation of data reading and writing, so as to realize the load balance of the server. At the same time, in the teaching and examination separation platform, the deployment mode of one master and two slaves is configured, which has obvious advantages and remarkable effects.

Keywords: MySQL; master-slave synchronization; load balancing; high availability

随着互联网的快速发展，MySQL作为一个开源的数据库平台，在互联网企业中，作为Web应用的数据存储解决方案，以其简单、高效、可移植性等特点深受用户的喜爱，得到了广泛的应用。数据库作为Web应用系统的核心组成部分，直接影响了整个应用系统的性能，随着用户数量的增加，普遍面临着高并发、大流量、高可用及海量数据的问题[1]。为了解决这些问题，大多企业采用数据库异步集群（MySQL Replication），实现读写分离，减轻数据库服务器的读写压力。

1 MySQL集群概述

1.1 主从复制

MySQL内建的复制功能是构建大型、高性能应用程序的基础。将MySQL的数据分布到多个系统上，这种分布的机制是通过将MySQL的某一台主机（Master）的数据复制到其他主机（Slave）上，并重新执行一遍来实现。复制过程中一个服务器充当主服务器，而一个或多个其他服务器充当从服务器[2]。

MySQL复制技术有数据分布、负载平衡、备份、高可用性和容错性等特点。MySQL支持的复制类型有以下三种：基于语句的复制，在主服务器上执行SQL语句，在从服务器上执行同样的语句，MySQL默认采用基于语句的复制，效率较高；基于

[收稿日期] 2022-04-19

[作者简介] 吴锋珍（1979—），男，福建长汀人，福建水利电力职业技术学院讲师，工程硕士，研究方向：计算机应用、数据库。

[基金项目] 2021年福建水利电力职业技术学院教科研课题“基于主从同步的MySQL负载均衡设计与部署”（课题编号：YJKJ2106B）。

行的复制，把改变的内容复制过去，而不是把命令在从服务器上执行一遍，从MySQL 5.0版本开始支持该复制类型；混合类型的复制，默认采用基于语句的复制，一旦发现基于语句无法精确复制，就会采用基于行的复制。

从整体上来说，复制有三个步骤：Master将改变记录到二进制日志（Binary Log）中，这些记录称为二进制日志事件（Binary Log Events）；Slave将Master的Binary Log Events复制到它的中继日志（Relay Log）中；Slave重做中继日志中的事件，改变它自己的数据。MySQL主从复制架构如图1所示。

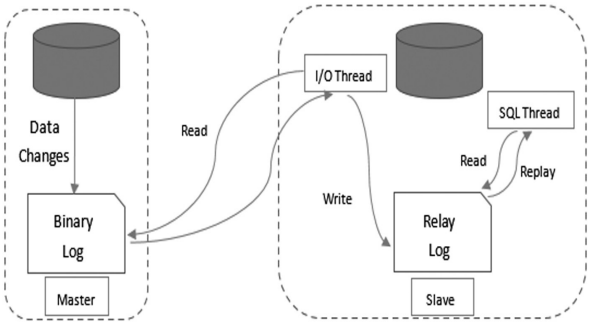

图1　MySQL主从复制架构图

1.2 读写分离

读写分离的基本原理是让主数据库处理事务性增加、删除、修改（Insert、Delete、Update）操作，而从数据库处理查询(Select)操作。数据库复制被用来把事务性操作导致的变更同步到集群中的从数据库。

因为数据库的“写”操作是比较耗时的，但数据库的“读”操作比较快，而且对数据库的操作中，更多的是“读”操作，所以读写分离可以解决数据库写入时影响查询效率的问题，从而提升数据库的并发负载能力[2]。但是只有解决了数据复制、数据同步、数据一致性等一系列问题，数据库的读写分离才能发挥它的高可用性、高并发性、负载均衡等作用。

2 环境与架构分析

在虚拟机下安装CentOS环境，借助各种开源软件进行服务器集群的部署实践。利用MyCat作为数据库中间件服务构建读写分离的数据库集群，MyCat将用户提交的读写操作分发给相应的数据库（MySQL）节点。这样将用户的访问操作、数据库的读和写操作分给三台服务器，只有数据库集群的主节点（Master）接收增、删、改操作，从节点（Slave）接收查询操作，分担了主节点的查询压力，加快用户请求的响应，提升用户体验，必要时可以设置多个Slave读库，来分担数据库的I/O压力[3]。实际的服务器架构如图2所示。

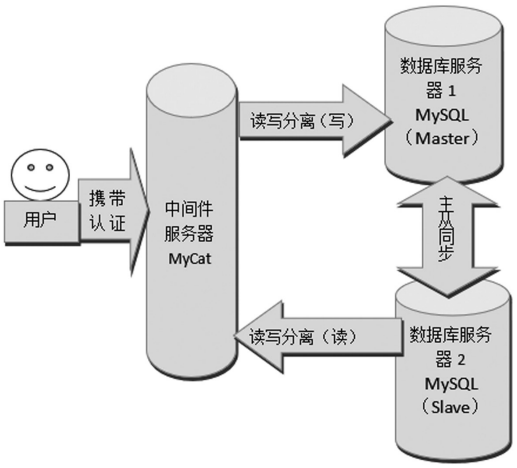

图2　服务器架构示意图

3 系统部署与实施

3.1 系统节点规划

该部署实践使用了三台服务器，对IP地址、主机名和节点的作用作如表1所示的规划。

表1　节点规划表

IP地址	主机名	节点
192.168.200.10	mycat	MyCat中间件服务节点
192.168.200.20	master	MySQL数据库集群主节点
192.168.200.30	slave	MySQL数据库集群从节点

3.2 系统部署与实施

3.2.1 基础环境配置

1）修改主机名，使用hostnamectl命令将三台主机的主机名分别修改为mycat、master和slave，如hostnamectl set-hostname mycat。

2）编辑hosts文件，在三台主机的/etc/hosts文件末尾添加如下三条件信息：

```
192.168.200.10      mycat
192.168.200.20      master
192.168.200.30      slave
```

3）配置YUM安装源，数据库集群需要安装MySQL数据库服务，需要给集群服务器配置YUM安装源文件，将MySQL安装包的文件mysql-repo上传至三台虚拟机的/opt目录下，设置本地YUM源。将三台主机的/etc/yum.repos.d/local.repo文件配置如下：

```
[mysql]
name=mysql
baseurl=file:///opt/mysql-repo
gpgcheck=0
enabled=1
```

3.2.2 部署MySQL主从数据库集群服务

1）安装MySQL服务，在master和slave虚拟机节点上安装MySQL服务，同时启动MySQL服务，并设置为开机自启动。

#yum install －y mysql mysql-server

#systemctl start mysql

#systemctl enable mysql

2）初始化MySQL数据库，在master和slave虚拟机节点上初始化MySQL数据库，并设置MySQL数据库root用户的密码为123123。

#mysql_secure_installation

在提示输入密码时，输入密码123123

Set root password?[Y/n]y #提示是否设置root用户密码,输入y

New password：#输入密码123123

Re-enter new password：#重复输入密码123123

3）配置数据库集群主节点，在主节点master虚拟机的数据库配置文件/etc/my.cnf文件中，添加如下内容：

[mysqld]

log_bin=mysql-bin #记录操作日志

binlog_ignore_db=mysql #不同步mysql系统数据库

server_id=20 #数据库集群中的每个节点id都不同，一般使用IP地址最后一段的数字。

4）开放主节点的数据库权限，在主节点master虚拟机上登录MySQL数据库，授权在任何客户端上可以以root用户登录到数据，命令如下：

Grant all privileges on *.* to root@'%' identified by "123123"；

同时创建一个user用户让从节点slave连接，并赋予从节点同步主节点数据库的权限，命令如下：

Grant replication slave on *.* to 'user'@'slave' identified by "123123"。

5）配置从节点同步主节点，在从节点slave虚拟机上登录MySQL数据库，配置从节点连接主节点的连接信息，命令如下：

Change master to master_host= ' master', master_user='user',

master_password='123123'；

配置完主从数据库之间的连接信息后，开启从节点服务。使用show slave status\G命令查看从节点服务状态，如果Slave_IO_running和Slave_SQL_running的状态都为Yes，则从节点服务开启成功[4]。

6）验证主从数据库的同步功能，先从主节点数据库中创建测试数据库(test)及数据表(tb_test)，并添加测试数据，然后从节点的数据就会同步主节点的数据库及数据，在从节点上可以查询到测试数据，说明主从数据库集群功能正常运行。

3.2.3 部署Mycat读写分离中间件服务

1）安装MyCat服务，将MyCat服务的二进制软件包MyCat-server-1.6-linux.tar.gz上传到MyCat虚拟机的/root目录下，并将软件包解压到/usr/local目录中，并赋予解压后的MyCat目录权限。同时，在/etc/profile系统变量文件中添加MyCat服务的系统变量，使之生效。

2）编辑MyCat的逻辑库配置文件，配置MyCat服务读写分离的schema.xml文件在/usr/local/mycat/conf/目录下，可以在文件中定义一个逻辑库，使用户可以通过MyCat服务管理该逻辑库对应的MySQL数据库。在这里定义一个名为schema的逻辑库，name为userdb，对应的数据库为在配置主从数据库服务集群中创建的测试数据库test,设置数据库写入节点为主节点master，读取节点为从节点slave。schema.xml文件的核心内容如下[2]：

<schema name=”userdb” checkSQLschema=” true” sqkNaxLimit= ” 100” dataNode= ” dn1” ></schema>

<writeHost host=”hostM1” url=”192.168.200.20:3306” user=”root” password=”123123”>

<readHost host=”hostS1” url=”192.168.200.30:3306” user=”root” password=”123123”/>

</ writeHost>

3）编辑MyCat的访问用户，修改/usr/local/mycat/conf/目录下的server.xml文件，修改root用户的访问密码为123123与逻辑库为userdb，内容如下：

<user name=”root”>

<property name=”password”>123123</property>

<property name=”schemas”>userdb</property>

</user>

4）启动MyCat服务，通过命令#/bin/bash/usr/local/mycat/bin/

mycat start启动MyCat数据库中间件服务，启动后使用netstat －ntpl命令查看虚拟机端口开放情况，如果开放了8066和9066端口，则表示MyCat服务开启成功。

3.2.4 验证数据库集群服务读写分离功能

1）通过MyCat服务查询数据库信息，先在MyCat虚拟机上使用YUM命令安装MySQL-Client

服务，并使用MySQL命令（#mysql －h127.0.0.1 －P8066 －uroot －p123123）登录MyCat服务，查看逻辑库userdb，可以查看到test数据库及对应tb_test数据表。

2）通过MyCat服务添加表数据，在MyCat虚拟机上使用insert命令对tb_test数据表添加一条测试数据，然后使用select命令查看数据表中的数据信息。

3）验证MyCat服务对数据库读写操作的分离，在MyCat虚拟机上使用MySQL命令，通过9066端口查询对数据库读写操作的分离信息。可以看到所有的写操作都在master主数据库节点上，所有的读操作都在slave从数据库节点上。由此可见，数据库的读写操作已经被分离，命令如下[2]：

#mysql －h127.0.0.1 －P9066 －uroot －p123123 －e ‘show @@datasource;’

查询的结果如表2所示：

表2　数据库读写分离查询结果表

Datanode	name	type	host	port	W/R	Read_load	Write_load
Dn1	hostM1	MySQL	192.168.200.20	3306	W	0	1
Dn1	hostS1	MySQL	192.168.200.30	3306	R	4	0

4 读写分离在教考分离平台的应用

在教考分离平台中，以往的部署形势都是Web服务器和MySQL数据库部署在一台物理服务器上，一台服务器承担着数据库的读和写操作，一般只能供两个班级的同学同时进行在线考试。随着学生数量的大幅增加，系统在抽题、学生提交等大量数据库访问操作时，系统运行缓慢。为了解决上述问题，对数据库服务器和Web服务器进行分离，同时对数据库服务器进行集群部署，配置一主两从，教考分离平台可以容纳七、八个班级的同学同时进行在线考试，而且抽题速度基本上不受影响。

接口响应速率、CPU 占有率和磁盘 I /O 是系统可用性高的重要性能指标，教考平台从这三个方面展开进行测试验证[5]，结果与前面的部署方式进行比较，也得到了明显提升。

5 总结

随着用户数量和数据量的增加，数据存储的可用性正在接受考验，通过数据库的集群技术，把数据库部署在不同的服务器上，实现读写分离，主从复制，甚至互为主从或一主多从，这样既实现了数据的安全性，也保证了系统的高可用性，从而实现了服务器的负载均衡。增加读库可以大幅提升主数据库的事务处理能力，从而大幅提高整个系统的业务承载能力[6]。

【参考文献】

[1]魏斌.高性能MySQL集群部署[J].河南科技,2014(14)：6-9.
[2]南京第五十五所技术开发有限公司.云计算平台运维与开发[M].北京：高等教育出版社，2020.
[3]丘杰雄.Nginx+Keepalived+Tomcat+MySQL高可用负载均衡Web应用架构实践[J].金融科技时代,2019(11)：38-42.
[4]刘进京.MySQL主从复制读写分离[J].网络安全和信息化，2016(4)：64-69.
[5]耿晓利，张芒，尹永宏.高并发高可用的分布式电商平台架构研究[J].计算机技术与发展，2021(2)：111-115,121.
[6]沙光华,陈泳,张长江.读写分离技术在运营支撑系统中的应用[J].计算机工程与应用,2015(12)：107-110,175.

（上接第36页）

复杂性，同时减轻与证书流程相关的管理工作；二是方案符合相关政策规范要求，满足移动应用系统扩展和进行商用密码算法升级改造的需求，应用无需关心密码运算和密码设备的使用细节，通过密码服务平台提供标准的密码服务接口即可实现，不受密码硬件设备等基础设施变动的影响；三是密码服务平台具有密码运营管理服务功能，可以满足企业后续根据业务需求对外提供密码运营和管理服务的需要。

【参考文献】

[1]杨晶，周海鑫.政务信息共享数据安全中的密码支撑技术与应用[J].信息安全与通信保密，2021(6):16-23.
[2]霍炜.商用密码应用体系建设与创新发展[J].信息安全研究,2020(11):958-965.
[3]工业和信息化部.2021年基础电信企业行业数据安全标准贯标工作方案[Z].工信厅网安函〔2021〕132号.
[4]林璟锵，荆继武.密码应用安全的技术体系探讨[J].信息安全研究，2019(1):14-22.
[5]潘玥琦.重庆市公路水运工程建设安全生产监管监信息系统研究[D].重庆：重庆交通大学，2018.